(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
7. September 2001 (07.09.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/65798 A1

(51) Internationale Patentklassifikation[7]: H04L 29/06

(21) Internationales Aktenzeichen: PCT/CH00/00116

(22) Internationales Anmeldedatum:
29. Februar 2000 (29.02.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SWISSCOM MOBILE AG** [CH/CH]; Schwarztorstrasse 61, CH-3050 Bern (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HUBER, Adriano** [CH/CH]; Via F. Caponelli, 35, CH-6600 Locarno (CH).

(74) Anwalt: **SAAM, Christophe**; Patents & Technology Surveys SA (AG, Ltd), 2 faubourg du Lac, P.O. Box 1448, CH-2001 Neuchâtel (CH).

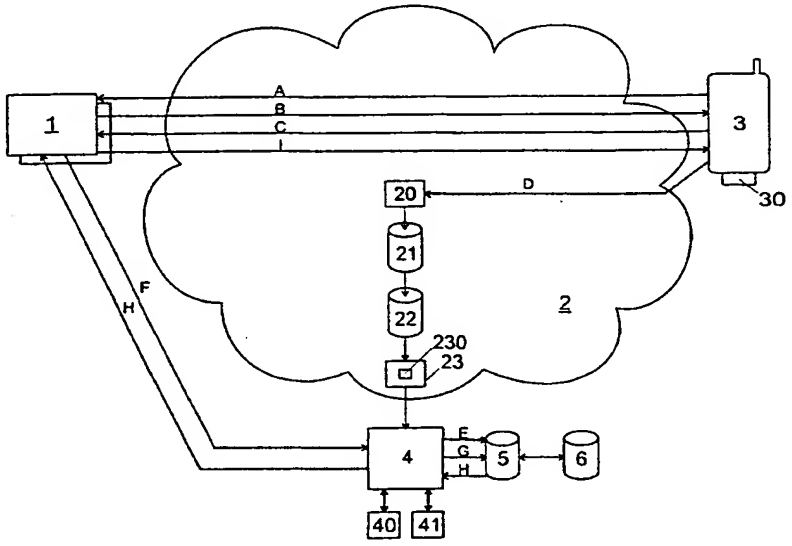
(81) Bestimmungsstaaten *(national)*: AE, AL, AM, AT, AT (Gebrauchsmuster), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), DM, EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Gebrauchsmuster), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI,

[Fortsetzung auf der nächsten Seite]

(54) Title: TRANSACTION CONFIRMATION METHOD, AUTHENTICATION SERVER AND WAP SERVER

(54) Bezeichnung: VERFAHREN ZUR TRANSAKTIONSBESTAETIGUNG, AUTHENTIFIZIERUNGSSERVER UND WAP-SERVER



(57) Abstract: The invention relates to a method with which a mobile subscriber can confirm a transaction with a service offerer (1), in which: an offer of said service offerer is reproduced by the mobile device (3) of said mobile subscriber; the mobile subscriber selects the offer using input means of his mobile device; a transaction confirmation is automatically routed from the mobile device to an authentication server (4), whereby a multitude of transactions between different mobile subscribers and different service offerers are stored in said authentication server, and; the service offerer retrieves the confirmation from the authentication server.

[Fortsetzung auf der nächsten Seite]

WO 01/65798 A1

FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Verfahren, mit welchem ein Mobilteilnehmer eine Transaktion mit einem Dienstanbieter (1) bestätigen kann, in welchem: ein Angebot des benannten Dienstanbieters wird mit dem Mobilgerät (3) des benannten Mobilteilnehmers wiedergegeben, der benannte Mobilteilnehmer selektiert das benannte Angebot mit Eingabemitteln seines Mobilgeräts, eine Transaktionsbestätigung wird automatisch vom benannten Mobilgerät an einen Authentifizierungsserver (4) geleitet, wobei eine Vielzahl von Transaktionen zwischen verschiedenen Mobilteilnehmern und verschiedenen Dienstanbietern im benannten Authentifizierungsserver gespeichert sind, und der benannte Dienstanbieter holt die benannte Bestätigung vom benannten Authentifizierungsserver ab.

VERFAHREN ZUR TRANSAKTIONSBESTAETIGUNG, AUTHENTIFIZIERUNGSSERVER UND WAP-SERVER

Die vorliegende Erfindung betrifft ein Verfahren, mit welchem ein Mobilteilnehmer eine Transaktion mit einem Dienstanbieter in einem Mobilfunknetz bestätigen kann.

Es sind schon verschiedene Verfahren bekannt, die es einem Mobilteilnehmer erlauben, eine Session mit einem Dienstanbieter herzustellen und Transaktionen durchzuführen, beispielsweise um Produkte oder Informationen zu bestellen oder um Geldtransaktionen durchzuführen. Mit WAP (Wireless Application Protocol) können beispielsweise sogenannte WAP-Karten von verschiedenen Dienstanbietern zur Verfügung gestellt werden und von Mobilteilnehmern mit geeigneten WAP-Browsern in WAP-tauglichen Mobilgeräten wiedergegeben werden. Auf jeder WAP-Karte können sich ein oder mehrere Angebote befinden, die vom Mobilteilnehmer mittels geeigneter Eingabemittel selektiert werden können, beispielsweise um ein Produkt oder eine Information zu bestellen.

Es wurde ausserdem auch beschrieben, wie man eine Web-Seite über ein Mobilfunknetz übertragen und auf einem Mobilgerät (beispielsweise einem Palmtop oder Laptop mit Funkschnittstelle) wiedergeben kann.

Will der Mobilteilnehmer eine Transaktion mit einem WAP- oder WEB-Dienstanbieter durchführen, muss er das entsprechende Angebot selektieren, beispielsweise durch anklicken des Angebots auf einer graphischen Oberfläche oder mit der Tastatur. Eine Transaktionsbestätigung wird dann automatisch vorbereitet und an den Dienstanbieter übertragen.

Damit der Dienstanbieter sicher sein kann, dass die Transaktionsbestätigung tatsächlich vom angegebenen Mobilteilnehmer gesendet wurde, muss ein Identifizierungsmechanismus vorgesehen werden. Zu diesem Zweck kann beispielsweise der Browser im Mobilgerät oder in der WIM-Karte des Mobilgeräts die Transaktionsbestätigung mit einem privaten Schlüssel signieren, der sich in einem von einer Drittinstanz

BESTÄTIGUNGSKOPIE

zertifizierten Zertifikat befindet. Der Dienstanbieter kann dann mit dem öffentlichen Schlüssel des Mobilteilnehmers dessen Signatur und auf diese Weise seine Identität prüfen.

Dieses Authentifizierungsverfahren kann jedoch erst eingesetzt werden, wenn das Mobilgerät des Mobilteilnehmers über Signierungsmittel verfügt, unter anderem über ein Zertifikat das von einer vom Dienstanbieter anerkannten Zertifizierungsinstanz zertifiziert wurde, sowie über ein geeignetes Signierungsmodul. Ausserdem muss der Dienstanbieter über den passenden öffentlichen Schlüssel des Mobilteilnehmers verfügen. Einfache oder ältere Mobilgeräte besitzen jedoch keine passenden Signierungsmittel. Ausserdem werden viele Zertifizierungsinstanzen nur national oder von bestimmten Benutzergruppen anerkannt, so dass dieses Verfahren nicht zwischen jedem Mobilteilnehmer und jedem Dienstanbieter eingesetzt werden kann.

Es ist ein Ziel der vorliegenden Erfindung, ein neues Bestätigungsverfahren für Transaktionen mit Mobilgeräten anzubieten.

Ein anderes Ziel ist es, ein neues Transaktionsbestätigungsverfahren anzubieten, das auch mit Mobilgeräten ohne Signierungsmodul und mit solchen Mobilgeräten eingesetzt werden kann, die über kein Zertifikat verfügen, das von einer vom Dienstanbieter anerkannten Zertifizierungsinstanz zertifiziert wurde.

Gemäss der vorliegenden Erfindung werden diese Ziele insbesondere durch die Merkmale der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Insbesondere werden diese Ziele durch ein Verfahren erreicht, in welchem die Transaktionsbestätigung automatisch vom Mobilgerät an einen Authentifizierungsserver geleitet wird, wobei eine Vielzahl von Transaktionen zwischen verschiedenen Mobilteilnehmern und verschiedenen Dienstanbietern im benannten Authentifizierungsserver gespeichert

sind. Der Dienstanbieter kann dann die Bestätigung vom benannten Authentifizierungsserver einholen.

Dies hat den Vorteil, dass sich Mobilteilnehmer für alle Transaktionen mit verschiedenen Dienstanbietern bei demselben Authentifizierungsserver identifizieren lassen können, anstatt für jeden Server jedes Dienstanbieters authentifizierbar sein zu müssen.

Wird der benannte Authentifizierungsserver vom Mobilfunknetzbetreiber oder von einem Betreiber mit einem Sonderabkommen mit dem Mobilfunknetzbetreiber verwaltet, können einfachere Authentifizierungsverfahren eingesetzt werden, die die im Identifikationsmodul im Mobilgerät gespeicherte Identität des Mobilteilnehmers verwenden.

In einer bevorzugten Variante besteht die benannte Bestätigung die vom benannten Mobilgerät gesendet wird aus einer USSD-Meldung, die aufgrund eines vorbestimmten Service Request Codes an einen bestimmten Authentifizierungsserver (beispielsweise an einen Server des Mobilfunknetzbetreibers) geleitet wird. Diese Variante erlaubt es, den Mobilteilnehmer einfach im HLR des Heimmobilfunknetzes zu identifizieren und diese Identität im Authentisierungsserver zu verwenden.

Im Folgenden werden anhand der beigefügten Zeichnungen bevorzugte Ausführungsbeispiele der Erfindung näher beschrieben:

Die Figur 1 zeigt ein Blockdiagramm, welches schematisch ein System darstellt, in welchem ein Mobilteilnehmer eine Transaktion mit einem Dienstanbieter mit einem Authentisierungsserver bestätigt.

Die Figur 2 zeigt schematisch die Struktur einer Bestätigungsmeldung, die von einem Mobilteilnehmer an den Authentisierungsserver gesendet wird.

Die Figur 3 zeigt schematisch die Struktur einer Bestätigungsmeldung, die im Authentisierungsserver gespeichert wird.

Obwohl diese Erfindung in mehreren Details den speziellen Fall der Ausführung in einem GSM-Mobilfunknetz beschreibt, wird der Fachmann verstehen, dass dieses Verfahren auch mit anderen Typen von Funknetzen, beispielsweise mit AMPS, TDMA, CDMA, TACS, PDC, HSCSD, GPRS, EDGE oder UMTS-Mobilfunknetzen eingesetzt werden kann, insbesondere mit WAP- (Wireless Application Protocol) fähigen Mobilfunknetzen. Diese Erfindung kann ausserdem in anderen Netzen, insbesondere im Internet oder in einem lokalen Netz gemäss Bluetooth oder HomeRF, verwendet werden.

In der Figur 1 bezieht sich die Bezugsziffer 1 auf einen Dienstanbieter (Service Provider), der ein Angebot (beispielsweise für ein Produkt oder eine Information) zur Verfügung stellt. Der Dienstanbieter betreibt vorzugsweise einen Server (beispielsweise einen http oder WAP-Server) in welchem HTML-Seiten (Hypertext Markup Language) beziehungsweise WML-Karten (Wireless Markup Language) gespeichert sind. Auf jeder Seite oder Karte können sich Text, Bilder und/oder Hypertext-Elemente befinden. Mindestens ein Element auf einer Seite oder Karte entspricht einem vom Mobilteilnehmer selektierbaren Angebot.

Jede Seite oder Karte besitzt eine Adresse, beispielsweise eine URL-Adresse (Uniform Resource Locator), im Telekommunikationsnetz 2. Das Telekommunikationsnetz 2 ist vorzugsweise ein Mobilfunknetz, (beispielsweise ein GSM oder UMTS-Mobilfunknetz, oder Internet, oder ein lokales Netz gemäss Bluetooth). Mobilteilnehmer können sich mit ihren Mobilgeräten 3 im Mobilfunknetz 2 anmelden und eine Session mit dem Dienstanbieter 1 herstellen, indem sie die benannte URL-Adresse in einen Browser im Mobilgerät 3 eingeben. Im Mobilfunknetz befinden sich mehrere Dienstanbieter 1 und mehrere Mobilgeräte 3.

Die Mobilgeräte 3 bestehen beispielsweise aus einem Rechner (z.B. Palmtop oder Laptop) mit einer Mobilfunkschnittstelle (beispielsweise mit einem Mobilgerät in PC-Card-Format oder mit einer kontaktlosen Schnittstelle zu einem Mobilfunktelefon) und aus einem WEB und/oder WAP-Browser, der HTML und/oder WML-Seiten wiedergeben kann.

Mindestens gewisse Mobilgeräte bestehen in einer bevorzugten Variante aus WAP-fähigen Mobilgeräten (beispielsweise aus Mobilfunktelefonen mit einem WML-fähigen Browser). Mobilgeräte 3 werden im Mobilfunknetz 2 anhand eines mit dem Mobilgerät verbundenen Identifizierungsmodul 30, beispielsweise anhand einer SIM- (Subscriber Identification Module), WIM- (WAP Identification Module) oder UIM- (UMTS Identification Module) Chipkarte, in welcher eine eindeutige und nicht verfälschbare Mobilteilnehmeridentifizierung, beispielsweise eine IMSI (International Mobile Subscriber Identification) abgelegt ist.

Das Mobilfunknetz 2 umfasst vorzugsweise mindestens eine Mobilvermittlungsstelle (MSC, Mobile Service Switching Center) 20, mindestens eine Besucherdatei (VLR, Visitor Location Register) 21 und mindestens eine Heimdatei (HLR, Home Location Register) 22. Die Heimdatei 22 wird von dem Netzbetreiber verwaltet, von welchem der Mobilfunkteilnehmer das Identifizierungsmodul 30 bezogen hat. Ein USSD-Handler 23 ist im HLR 22 enthalten oder mit ihm verbunden und prüft alle empfangenen USSD-Meldungen um zu entscheiden, welche Aktion damit ausgeführt werden soll. Ein Filter 230 in diesem USSD-Handler 23 erkennt unter anderem die für das erfindungsgemässe Verfahren angewandten und speziell markierten USSD-Meldungen und leitet sie an den Authentifizierungsserver 4 weiter, wie weiter unten beschrieben.

USSD-Meldungen (Unstructured Supplementary Service Data) wurden unter anderem beispielsweise im Standard GSM 02.90 vom European Telecommunications Standards Institute (ETSI) definiert und standardisiert.

Die Bezugsziffer 4 bezieht sich auf einen Authentifizierungsserver, beispielsweise auf einen UNIX, LINUX oder Windows-Server und wird beispielsweise vom Betreiber des Mobilfunknetzes 2 betrieben, oder von einer Instanz mit einem Sonderabkommen mit diesem Betreiber, damit speziell markierte USSD-Meldungen an ihn weitergeleitet werden. Der Server 4 enthält oder ist verbunden mit einer Datenbank 5, in welcher Transaktionsbestätigungen abgelegt werden. Eine zusätzliche Benutzer-

datenbank 6 enthält Benutzerangaben, beispielsweise Namen, Adresse, usw. Im Server können ausserdem verschiedene Anwendungen 40, 41,.., abgelegt werden, die beim Empfang einer bestimmten USSD-Meldung durchgeführt werden, wie weiter unten beschrieben. Der Server 4 kann beispielsweise einen http- oder FTP-Server enthalten und über einen nicht dargestellten Router mit dem Internet verbunden sein.

Jeder Dienstanbieter 1 kann über ein nicht dargestelltes geeignetes Telekommunikationsnetz (beispielsweise über Internet) auf den Server 4 zugreifen, um Transaktionen die ihn betreffen abzuholen, z.B. mit einem http oder CORBA-Protokoll. Die Sessionen zwischen den Dienstanbietern 1 und dem Server 4 werden vorzugsweise gesichert, beispielsweise gemäss dem Protokoll SSL (Secure Sockets Layer), TLS (Transport Layer Security) oder WTLS (Wireless Transport Layer Security). Der Authentifizierungsserver 4 verfügt ausserdem über nicht dargestellte Signierungsmittel, mit welchen Meldungen und Sessionen mit den Dienstanbietern 1 gesichert werden können.

Wir werden jetzt ein Beispiel des erfindungsgemässen Verfahrens das mit diesem System durchgeführt werden kann näher beschreiben.

Der Mobilteilnehmer kann sich mit dem Mobilgerät 3 ein Angebot des Dienstanbieters 1 darstellen lassen, indem er die URL-Adresse der entsprechenden WAP-Karte oder Web-Seite in seinen Browser eingibt (Pfeil A). Die WML bzw. HTML-Seite wird dann über das Telekommunikationsnetz 2 (beispielsweise über ein zellulares Mobilfunknetz oder Internet) übertragen (Pfeil B) und auf der Anzeige oder mit sonstigen Wiedergabemitteln des Mobilgeräts 3 vom Browser in einer geeigneten Form wiedergegeben. Die Sessionen zwischen dem Dienstanbieter 1 und dem Mobilteilnehmer 3 können gesichert sein oder nicht.

Die WAP-Karte bzw. Web-Seite kann beispielsweise ein oder mehrere Hyperlinkelemente oder andere graphische Bedienungselemente (beispielsweise anklickbare Knöpfe oder Selektionskasten) enthalten, die vom Mobilteilnehmer mit geeigneten Bedienungselementen selektiert

werden können, um das entsprechende Angebot auf der Karte oder Seite auszuwählen.

Sobald das Angebot selektiert worden ist, wird ein Skript erstellt, (beispielsweise ein WML, Java oder Javascript-Skript) das die Vorbereitung und Sendung einer USSD-Meldung veranlasst (Pfeil D). Die ganze USSD-Meldung wird vorzugsweise in dem mit der Web-Seite oder WAP-Karte übermittelten Skript angegeben; es ist jedoch auch möglich, dass mindestens gewisse Felder der USSD-Meldung vom Prozessor im Mobilgerät 3 oder im Identifizierungsmodul ermittelt werden (beispielsweise anhand von im Mobilgerät vorhandenen Angaben).

Die Struktur eines bevorzugten Beispiels von USSD ist auf der Figur 2 dargestellt. In diesem Beispiel enthält die USSD-Meldung von links nach rechts ein erstes Abgrenzungszeichen (in diesem Beispiel *#) gefolgt von einem dreistelligen Dienstcode SRQ. Gemäss den oben erwähnten Richtlinien GSM 02.90 kann der Dienstcode jeder mögliche Wert im Bereich von 100 bis 1999 sein. Der Dienstcode SRQ bestimmt, wohin die USSD-Meldung geleitet werden soll, insbesondere ob sie vom VLR in einem besuchten Mobilfunknetz oder vom HLR des Heimnetzes behandelt werden soll. Der Wert des SRQ-Feldes ist in dieser Anwendung für alle USSD festgelegt, damit alle Transaktionsbestätigungen als USSD an den Server 4 geleitet werden, wie später erläutert.

Ein zweites Abgrenzungszeichen wird nach dem Dienstcode SRQ verwendet (in diesem Beispiel ein *). Nach diesem Zeichen folgt ein Feld SP-Code mit einer Identifizierung des Dienstanbieters 1, vorzugsweise eine Identifizierung, die auch dem Betreiber des Netzes 4 bekannt ist, beispielsweise seine URL-Adresse oder der Titel der WAP-Karte oder Web-Seite, oder einfach eine Nummer.

Das nächste Feld TS1 enthält einen vom Dienstanbieter 1 gesetzten Zeitstempel, welcher das Datum und die Zeit der Übertragung der WAP-Karte oder Web-Seite angibt. Das Feld SES-ID enthält eine vom Dienst-

anbieter 1 definierte Identifizierung der Session durch das Netz 2, während welcher die WAP-Karte oder Web-Seite übermittelt wurde.

Das Feld Rd-Nr enthält ein Geheimnis vom Dienstanbieter (beispielsweise eine generierte Zufallnummer die für jede übertragene Kopie der WAP-Karte oder Web-Seite unterschiedlich ist und die vom Mobilteilnehmer nicht erraten werden kann).

Das Feld USER-D enthält im Mobilgerät 3 oder im Identifizierungsmodul 30 vorhandenen Angaben, beispielsweise die Identität (beispielsweise die IMSI) des Mobilteilnehmers, seine elektronische Signatur, seinen Standort, seine Sprache, seine Bestellungspräferenzen, usw. Es ist auch möglich, die USSD-Meldung mit Angaben aus einer externen Vorrichtung zum Beispiel aus einem POS (Point-of-Sale) im Nahbereich, zu ergänzen, die über eine kontaktlose Schnittstelle (bei gemäss Bluetooth, HomeRF oder IrdA) übertragen wurden. Die Identität des Mobilteilnehmers, sowie allenfalls andere Parameter, werden in einer bevorzugten Variante verschlüsselt.

Das Feld KEY enthält einen Verschlüsselungsschlüssel, mit welchem vom Mobilteilnehmer eingegebene oder vom Mobilgerät ermittelte Daten verschlüsselt werden können, um damit ein nur vom Dienstanbieter 1 entschlüsselbares Feld CYPHER zu ermitteln.

Zusätzliche Felder F1, F2, .. können ausserdem gesetzt werden, um bestimmte Anwendungen im Authentisierungsserver 4 durchführen zu lassen, wie später erläutert.

Der Fachmann wird verstehen, dass diese Struktur einer USSD-Meldung nur als Beispiel angegeben worden ist und dass zusätzliche Felder vorgesehen werden können während die hier beschriebenen Felder optional sind. Es ist beispielsweise durchaus denkbar, auch Datagramme zu senden, das heisst Meldungen mit Feldern, die ein ausführbares Programm oder Programmelement enthalten, beispielsweise mit einem JAVA-Applet (Warenzeichen von SUN Microsystems, Inc.)

Die im Mobilgerät 3 vorbereitete USSD-Meldung wird durch die Mobilvermittlungsstelle MSC 20, die Besucherdatei 21 (VLR, Visitor Location Register) und die Heimdatei 22 (HLR, Home Location Register) zum USSD-Handler 23 geleitet (Pfeil D), wo sie aufgrund des SRQ-Wertes vom Filtermodul 230 sortiert und zum Authentisierungsserver 4 weitergeleitet wird. Vorzugsweise wird vom benannten Script eine Bestätigung vorbereitet (Pfeil C), die mit einem geeigneten Bearer (E-Mail, SMS, usw..) direkt zum Dienstanbieter 1 gesendet wird, sobald der Mobilteilnehmer ein Angebot selektiert hat.

Im Authentisierungsserver 4 wird die USSD-Meldung empfangen und vorzugsweise mit zusätzlichen Feldern TS2 und/oder SIG2 ergänzt (Figur 3). Das Feld TS2 enthält einen Zeitstempel, der vom Authentisierungsserver beim Empfang der USSD-Meldung gesetzt wird und welcher das Empfangsdatum und die Empfangszeit angibt. Das Feld SIG2 enthält eine elektronische Signatur des Authentisierungsservers 4.

Der Authentisierungsserver 4 erfährt ausserdem vom USSD-Handler 23 die Identität des Mobilteilnehmers 3, beispielsweise seine IMSI. Der Fachmann wird feststellen, dass diese IMSI nicht verfälscht werden kann und dass es nicht möglich ist, eine USSD-Meldung mit der IMSI eines anderen Mobilteilnehmers zu senden. In einer bevorzugten Variante werden diese Benutzerangaben mit zusätzlichen Angaben aus einer Benutzerdatenbank 6 verknüpft, beispielsweise mit der Rechnungs- und/oder Lieferungsadresse.

Der Authentisierungsserver 4 legt dann die ergänzte Meldung in einer Transaktionsdatenbank 5 ab (Pfeil E), in welcher eine Vielzahl von Transaktionen zwischen verschiedenen Dienstanbietern und verschiedenen Mobilteilnehmern abgelegt werden. In der Datenbank 5 wird vorzugsweise ein Index auf das Feld SP-Code aufgebaut, damit die abgelegten Daten schnell nach Dienstanbieter sortiert werden können.

Verschiedene Anwendungen 40, 41, .. im Server 4 können ausserdem durchgeführt werden, wenn ein Flag F1, F2, .. gesetzt ist oder wenn

besondere Bedingungen erfüllt sind, um eine bestimmte Aktion auszulösen. Wird der Server 4 vom Betreiber des Mobilfunknetzes 2 betrieben, ist es beispielsweise möglich, einem Konto des Mobilteilnehmers 3 und/oder des Dienstanbieters 1 eine Gebühr zu belasten.

Die Dienstanbieter 1 können eine Anfrage F an den Server 4 senden, um zu prüfen, ob Transaktionsbestimmungen in der Datenbank 5 abgelegt wurden. Anfragen können beispielsweise periodisch, nach Empfang der Bestätigung C oder nach einer vorbestimmten Zeit nach dem Fernladen der einer WAP-Karte oder Web-Seite gesendet werden. Die Anfrage wird beispielsweise durch Internet oder durch ein Mobilfunknetz während einer vorzugsweise gesicherten Session übertragen. Im Authentisierungsserver 4 wird vorzugsweise die Identität des Dienstanbieters 1 geprüft (beispielsweise anhand von bekannten Authentisierungsmechanismen mit elektronischen Signaturen, mit einem Passwort oder allgemein mit einem geteilten Geheimnis) und die Zugriffsberechtigung des Dienstanbieters 1 auf den Inhalt der Transaktionsdatenbank 5 wird getestet. Ist das Ergebnis dieser Prüfung positiv, wird die Anfrage an die Transaktionsdatenbank 5 weitergeleitet (Pfeil G), die mit der auf der Figur 3 dargestellten Transaktionsbestätigung antwortet (Pfeil H). Diese Antwort wird dann vorzugsweise vom Server 4 elektronisch signiert und/ oder verschlüsselt und an den Dienstanbieter 1 weitergeleitet (Pfeil H).

In einer Variante der Erfindung wird die Benutzeridentifizierung (USER-D) aus der Antwort (Pfeil H) entfernt, damit der Benutzer gegenüber dem Dienstanbieter anonym bleibt. Auf diese Weise können auch für den Dienstanbieter 1 anonyme Zahlungen durchgeführt werden.

In einer Variante der Erfindung muss der Dienstanbieter nicht selbst Anfragen an den Authentifizierungsserver 4 senden, sondern wird von ihm informiert, wenn eine Transaktionsbestätigung angekommen ist. Zu diesem Zweck kann ein Script im Server 4 vorgesehen werden, das Bestätigungen, oder vorzugsweise nur speziell markierte Bestätigungen, automatisch an den entsprechenden Dienstanbieter weiterleitet.

Der Dienstanbieter kann dann aufgrund der empfangenen Bestätigung den Mobilteilnehmer zuverlässig identifizieren. Anhand der Sessions-Identifizierung SES-ID, des Zeitstempels TS1, der Zufallsnummer Rd-Nr und eventuell der anderen vom Mobilgerät 3 und/oder vom Server 4 gesetzten Felder kann er ausserdem prüfen, ob die empfangenen Daten wirklich einer von ihm gesendeten WAP-Karte oder Web-Seite entsprechen.

Auf diese Weise kann der Dienstanbieter 1 sicher sein, dass wirklich der Mobilteilnehmer 3 der Ursprung der empfangenen Bestätigung ist und kann somit die Transaktion durchführen, indem beispielsweise ein bestelltes Produkt gesendet wird und/oder indem die angebotene Information über das Mobilfunknetz 2 gesendet wird. Vorzugsweise wird dem Mobilteilnehmer eine Bestätigung gesendet (Pfeil I).

Der Fachmann wird verstehen, dass im Rahmen dieser Erfindung auch andere Meldungen als USSD-Meldungen verwendet werden können. Ausserdem ist es möglich, mehrere Authentisierungsserver 4 einzusetzen, die beispielsweise mit anderen SRQ-Codes erreicht werden. Auf diese Weise kann ein Dienstanbieter durch Auswahl eines anderen SRQ-Codes entscheiden, in welchen Authentisierungsserver 4 die Authentisierungsdaten für eine bestimmte Transaktion abgelegt werden sollen.

Die Verwendung des Authentisierungsservers 4 kann beispielsweise im Rahmen von Benutzerverträgen zwischen dem Betreiber des Servers 4 und den Dienstanbietern 1 fakturiert werden, wobei der verrechnete Preis beispielsweise von der Anzahl der empfangenen Transaktionen abhängig sein kann. Zu diesem Zweck kann ein Transaktionszähler im Server 4 vorgesehen werden, welcher während einer vordefinierten Zeitspanne für jeden Dienstanbieter 1 die Anzahl von Transaktionen zählt.

Vorzugsweise wird ein Profil für jeden registrierten Dienstanbieter 1 im Server 4 gespeichert, in welchem unter anderem die Identität des Dienstanbieters, der entsprechende SP-Code, eventuell seine Rechnungsadresse und eventuelle Präferenzen (beispielsweise über die Art wie

die Transaktionsbestätigungen in der Transaktionsdatenbank 5 abgelegt werden sollen) gespeichert sind.

Ansprüche

1. Verfahren, mit welchem ein Mobilteilnehmer eine Transaktion mit einem Dienstanbieter (1) bestätigen kann, dadurch gekennzeichnet,
dass ein Angebot des benannten Dienstanbieters (1) mit dem Mobilgerät (3) des benannten Mobilteilnehmers wiedergegeben wird,
dass der benannte Mobilteilnehmer das benannte Angebot mit Eingabemitteln seines Mobilgeräts (3) selektiert,
dass eine Transaktionsbestätigung automatisch vom benannten Mobilgerät an einen Authentifizierungsserver geleitet wird (D), wobei eine Vielzahl von Transaktionen zwischen verschiedenen Mobilteilnehmern (3) und verschiedenen Dienstanbietern (1) im benannten Authentifizierungsserver (4) gespeichert sind,
und dass der benannte Dienstanbieter (1) die benannte Bestätigung vom benannten Authentifizierungsserver einholen kann (F-H).

2. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass das benannte Angebot in einer WAP-Karte des benannten Dienstanbieters enthalten ist, die von einem Browser im benannten Mobilgerät (3) wiedergegeben wird.

3. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass das benannte Angebot in einer Web-Seite enthalten ist, die von einem Browser im benannten Mobilgerät (3) wiedergegeben wird.

4. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung, die vom benannten Mobilgerät (3) gesendet wird, aus einer USSD-Meldung besteht.

5. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannte USSD-Meldung automatisch von einem Script das in der benannten WAP-Karte oder Web-Seite enthalten ist vorbereitet und gesendet wird, wenn der benannte Mobilteilnehmer ein Angebot auf dieser Karte bzw. Seite selektiert.

6. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das benannte Script ein WML-Script ist.

7. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung eine Dienstanbieteridentifizierung (SP-Code) enthält.

8. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung einen Zeitstempel (TS1) vom benannten Dienstanbieter (1) enthält.

9. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung eine Sessionsidentifizierung (SES-ID) enthält.

10. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung ein nur dem Dienstanbieter (1) bekanntes Geheimnis (Rd-Nr) enthält.

11. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das benannte Geheimnis (Rd-Nr) eine vom benannten Dienstanbieter festgelegte Zufallsnummer ist.

12. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung eine Benutzeridentifizierung enthält.

13. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens ein Teil der benannten Bestätigung durch ein Script im benannten Mobilgerät (3) vorbereitet wird.

14. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens ein Teil (USER-D) der benannten Bestätigung durch ein Script im benannten Mobilgerät mit einem Schlüssel (KEY) des Dienstanbieters (1) verschlüsselt wird.

15. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung ein Datagramm, das vom benannten Authentifizierungsserver durchgeführt wird, enthält.

16. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung mindestens ein Flag (F1, F2, ..), das die Durchführung einer Anwendung im benannten Authentifizierungsserver (4) verursacht, enthält.

17. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung in einer Transaktionsdatenbank (5) im benannten Authentifizierungsserver (4) abgelegt wird.

18. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass der benannte Authentifizierungsserver (4) eine Benutzerdatenbank (6) enthält, in welcher Mobilteilnehmerangaben abgelegt sind,

und dass mindestens gewisse dieser Mobilteilnehmerangaben mit der benannten Bestätigung im benannten Authentifizierungsserver (4) verknüpft werden.

19. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung vom benannten Authentifizierungsserver (4) elektronisch signiert wird.

20. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung vom benannten Authentifizierungsserver beim Empfang mit einem Zeitstempel (TS2) versehen wird.

21. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannte Bestätigung im benannten Authentifizierungsserver (4) abgelegt wird und dass der benannte Dienst-

anbieter (1) eine Anfrage an den benannten Authentifizierungsserver (4) sendet (F), um zu prüfen, ob die Bestätigung angekommen ist.

22. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass der benannte Authentifizierungsserver (4) einen http-Server umfasst und dass sich der benannte Dienstanbieter (1) über Internet mit dem benannten Authentifizierungsserver verbindet, um zu prüfen, ob eine Bestätigung angekommen ist.

23. Verfahren gemäss einem der Ansprüche 21 oder 22, dadurch gekennzeichnet, dass sich der benannte Dienstanbieter beim benannten Authentifizierungsserver (4) elektronisch authentifizieren lassen muss, um Bestätigungen abzuholen.

24. Verfahren gemäss einem der Ansprüche 1 bis 20, dadurch gekennzeichnet, dass die benannte Bestätigung automatisch vom benannten Authentifizierungsserver (4) an den benannten Dienstanbieter weitergeleitet wird.

25. Verfahren gemäss einem der Ansprüche 21 bis 24, dadurch gekennzeichnet, dass der benannte Dienstanbieter eine Bestätigung (I) an den benannten Mobilteilnehmer sendet, sobald er die benannte Bestätigung (H) vom benannten Authentifizierungsserver eingeholt hat.

26. WAP-Server (1), in welchem WAP-Karten abgelegt sind, die von einer Vielzahl von Mobilteilnehmern mit WAP-tauglichen Mobilgeräten (3) abgeholt werden können, wobei mindestens gewisse benannte WAP-Karten Angebote enthalten, dadurch gekennzeichnet, dass mindestens gewisse WAP-Karten ein WML-Script umfassen, mit welchem eine Transaktionsbestätigung als USSD an einen vorbestimmten Authentifizierungsserver (4) gesendet wird, wenn ein benanntes Angebot mit einem WAP-Browser in einem benannten Mobilgerät (3) selektiert wird.

27. WAP-Server gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten USSD eine Dienstanbieteridentifizierung (SP-Code) enthalten.

28. WAP-Server gemäss einem der Ansprüche 26 bis 27, dadurch gekennzeichnet, dass die benannte WAP-Karte einen Zeitstempel (TS1) umfasst, welcher die Fernladezeit der WAP-Karte bestimmt und dass das benannte Script eine Kopie dieses Zeitstempels in die benannten USSD macht.

29. WAP-Server gemäss einem der Ansprüche 26 bis 28, dadurch gekennzeichnet, dass die benannten USSD eine Sessionsidentifizierung (SES-ID) enthalten.

30. WAP-Server gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannten USSD ein nur dem Dienstanbieter bekanntes Geheimnis (Rd-Nr) enthalten.

31. WAP-Server gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das benannte Geheimnis (Rd-Nr) eine vom benannten Dienstanbieter (1) festgelegte Zufallsnummer ist.

32. Authentifizierungsserver (4), der mit einem Mobilfunknetz (2) derart verbunden ist, dass USSD-Meldungen mit einem vorbestimmten USSD Service Request Code an ihn geleitet werden, dadurch gekennzeichnet, dass er eine Transaktionsdatenbank (5) enthält, in welcher Transaktionsbestätigungen die in den benannten USSD enthalten sind abgelegt werden, wobei eine Vielzahl von Transaktionen zwischen verschiedenen Mobilteilnehmern (3) und verschiedenen Dienstanbietern (1) empfangen und gespeichert werden.

33. Authentifizierungsserver gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass er einen http-Server umfasst, mit welchem sich benannte Dienstanbieter (1) über Internet verbinden können, um zu prüfen, ob eine Bestätigung angekommen ist.

34. Authentifizierungsserver gemäss einem der Ansprüche 32 oder 33, dadurch gekennzeichnet, dass er ein Authentifizierungsmodul umfasst, das die benannten Dienstanbieter (1) authentifizieren kann, bevor diese Bestätigungen einholen können.

35. Authentifizierungsserver gemäss einem der Ansprüche 32 bis 34, dadurch gekennzeichnet, dass er mindestens ein Anwendungsprogramm (40, 41, ..) enthält, das ausgeführt wird wenn ein bestimmtes Flag (F1, F2, ..) in ankommenden USSD gesetzt ist.

36. Authentifizierungsserver gemäss einem der Ansprüche 32 bis 35, dadurch gekennzeichnet, dass er eine Benutzerdatenbank (6) enthält, in welcher Mobilteilnehmerangaben abgelegt sind,
und dass mindestens gewisse dieser Mobilteilnehmerangaben mit der benannten Bestätigung verknüpft werden.

37. Authentifizierungsserver gemäss einem der Ansprüche 32 bis 36, dadurch gekennzeichnet, dass die ankommenden USSD elektronisch signiert werden.

38. Authentifizierungsserver gemäss einem der Ansprüche 32 bis 37, dadurch gekennzeichnet, dass die ankommenden USSD mit einem Zeitstempel (TS2) versehen werden.

39. Authentifizierungsserver gemäss einem der Ansprüche 32 bis 38, dadurch gekennzeichnet, dass er ein Profil für jeden registrierten Dienstanbieter 1 enthält.

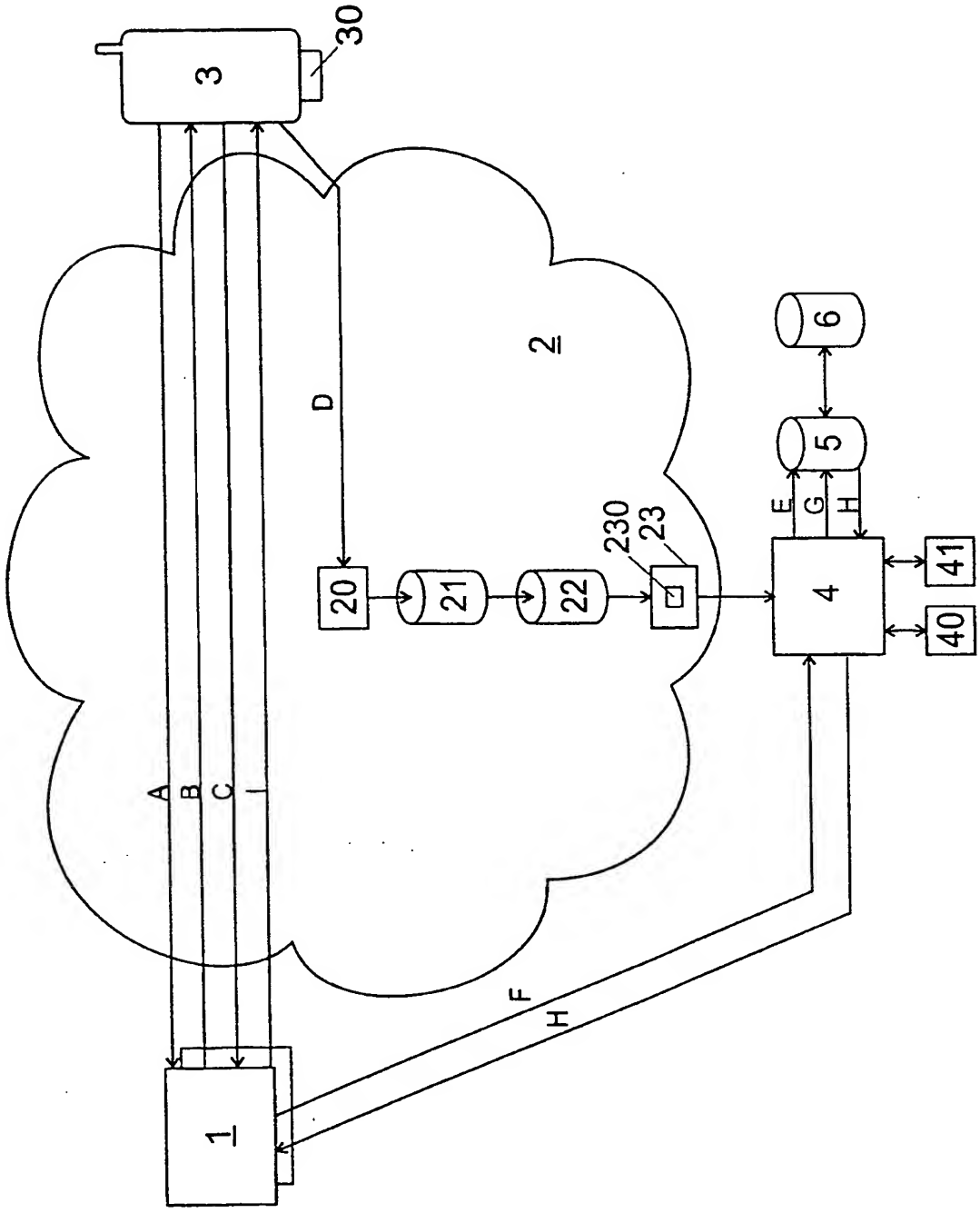


Fig. 1

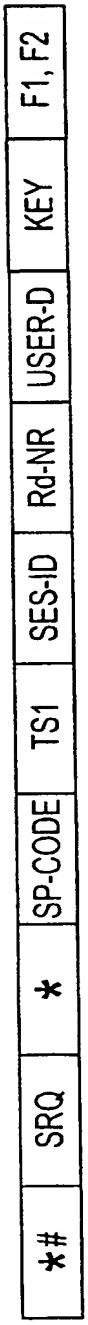

*#
SRQ
*
SP-CODE
TS1
SES-ID
Rd-NR
USER-D
KEY
F1, F2

Fig. 2

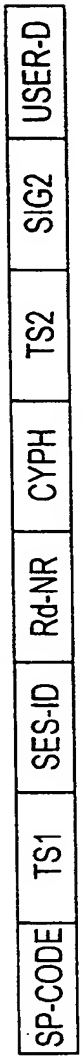

SP-CODE
TS1
SES-ID
Rd-NR
CYPH
TS2
SIG2
USER-D

Fig. 3

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/CH 00/00116

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 813 325 A (AT & T CORP) 17 December 1997 (1997-12-17) abstract column 2, line 29 -column 5, line 46	1,26,32
A	WO 99 56434 A (ERICSSON TELEFON AB L M) 4 November 1999 (1999-11-04) page 1, line 14 -page 2, line 20 page 5, line 6 -page 6, line 17 page 9, line 4 -page 11, line 9 page 17, line 30 -page 19, line 31	1,26,32
A	US 5 883 810 A (ROSEN DANIEL ET AL) 16 March 1999 (1999-03-16) column 3, line 48 - line 59 column 6, line 1 - line 11 column 7, line 28 - line 32 column 8, line 15 -column 11, line 45	1,26,32

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 April 2001	10/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kesting, V

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/CH 00/00116

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HOOGENBOOM M ET AL: "Security For Remote Access And Mobile Applications" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 19, no. 2, February 2000 (2000-02), pages 149-163, XP004204675 ISSN: 0167-4048 page 154, left-hand column, line 31 -page 161, left-hand column, line 17	1,26,32

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna. al Application No
PCT/CH 00/00116

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0813325 A	17-12-1997	US 5778173 A	07-07-1998
		CA 2205124 A	12-12-1997
		JP 10149397 A	02-06-1998
WO 9956434 A	04-11-1999	FI 980952 A	30-10-1999
		AU 3418399 A	16-11-1999
		EP 1075748 A	14-02-2001
US 5883810 A	16-03-1999	NONE	

INTERNATIONALER RECHERCHENBERICHT

Interna ales Aktenzeichen
PCT/CH 00/00116

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 813 325 A (AT & T CORP) 17. Dezember 1997 (1997-12-17) Zusammenfassung Spalte 2, Zeile 29 -Spalte 5, Zeile 46 ---	1,26,32
A	WO 99 56434 A (ERICSSON TELEFON AB L M) 4. November 1999 (1999-11-04) Seite 1, Zeile 14 -Seite 2, Zeile 20 Seite 5, Zeile 6 -Seite 6, Zeile 17 Seite 9, Zeile 4 -Seite 11, Zeile 9 Seite 17, Zeile 30 -Seite 19, Zeile 31 ---	1,26,32
A	US 5 883 810 A (ROSEN DANIEL ET AL) 16. März 1999 (1999-03-16) Spalte 3, Zeile 48 - Zeile 59 Spalte 6, Zeile 1 - Zeile 11 Spalte 7, Zeile 28 - Zeile 32 Spalte 8, Zeile 15 -Spalte 11, Zeile 45 --- -/--	1,26,32

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategonen von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
3. April 2001	10/04/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kesting, V

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internes Aktenzeichen
PCT/CH 00/00116

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	HOOGENBOOM M ET AL: "Security For Remote Access And Mobile Applications" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, Bd. 19, Nr. 2, Februar 2000 (2000-02), Seiten 149-163, XP004204675 ISSN: 0167-4048 Seite 154, linke Spalte, Zeile 31 -Seite 161, linke Spalte, Zeile 17	1,26,32

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interna. les Aktenzeichen
PCT/CH 00/00116

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0813325 A	17-12-1997	US 5778173 A	07-07-1998
		CA 2205124 A	12-12-1997
		JP 10149397 A	02-06-1998
WO 9956434 A	04-11-1999	FI 980952 A	30-10-1999
		AU 3418399 A	16-11-1999
		EP 1075748 A	14-02-2001
US 5883810 A	16-03-1999	KEINE	